אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

המחלקה למדעי המחשב

דר' עמוס ביימל

קריפטוגרפיה - מועד א'

202-1-5351

סמסטר ב' תשס"ב

10.7.2002

הנחיות:

1. בטופס הבחינה שני דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 4 שאלות שמשקלן אינו שווה. יש לענות על כולן.
3. הבחינה עם חומר פתוח.
4. נמקו את כל תשובותיכם. פתרון ללא הוכחה לא יתקבל.
5. משך הבחינה 3 שעות.
6. מומלץ לא להיתקע זמן רב מדי על שום סעיף.
7. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.

בהצלחה!

שאלה 1 [20 נקודות]

בשאלה זו נראה כשל נוסף במערכת ההצפנה RSA כאשר משתמשים בה בצורה שגויה. לשם פשטות נתייחס למקרה בו $e=3$. כלומר, המפתח הציבורי הוא $(N,3)$ כאשר N הוא מכפלה של שני ראשוניים גדולים שונים זה מזה ו- $\gcd(3,\varphi(N))=1$. נניח כי עבור הודעה כלשהי $m \in \mathbb{Z}_N^*$ אליס מצפינה את m ואת $m+1$, כלומר מחשבת $c_1 \leftarrow m^3 \bmod N$ ו- $c_2 \leftarrow (m+1)^3 \bmod N$.

איב מאזינה לערוץ השידור, יודעת מהו המפתח הציבורי ויודעת כי קיימת הודעה m כך שאליס הצפינה את m ואת $m+1$. בשאלה זו תראו איך איב יכולה למצוא בצורה יעילה את m.

סעיף א [7 נקודות]

הראו איך איב יכולה בצורה יעילה לחשב את $(3m^2+3m+3) \bmod N$ כאשר נתונים לה c_1, c_2 ו- N בלבד.

סעיף ב [8 נקודות]

הראו איך איב יכולה בצורה יעילה לחשב את $(3m^3+3m^2+3m) \bmod N$ כאשר נתונים לה c_1, c_2 ו- N בלבד.

סעיף ג [5 נקודות]

הראו איך איב יכולה בצורה יעילה לחשב את m כאשר נתונים לה c_1, c_2 ו- N בלבד.

שאלה 2 [34 נקודות]

בשאלה זו נראה כי יש לבחור בזהירות את מפתח החתימה במערכת החתימה של ElGamal. יהי p ראשוני ו- w שלם כך ש- $p=2w+1$. נניח כי 2 ו- w הם יוצרים של $\mathbb{Z}_p^*$.

סעיף א [7 נקודות]

הראו כי 2 ו- 6 הם יוצרים של $\mathbb{Z}_{13}^*$.

סעיף ב [6 נקודות]

הראו כי לכל $x \in \mathbb{Z}_p^*$ מתקיים $x^w \equiv 1 \pmod p$ או $x^w \equiv -1 \pmod p$.

סעיף ג [8 נקודות]

הראו כי $w^{w-1} \equiv 2 \pmod p$.

סעיף ד [5 נקודות]

יהי $(p,2,B)$ מפתח ציבורי במערכת החתימה של ElGamal. הראו איך למצוא ביעילות z כך ש- $2^{wz} \equiv B^w \pmod p$.

סעיף ה [8 נקודות]

יהי $m \in \mathbb{Z}_p^*$ מסמך כלשהו. נגדיר $\delta \leftarrow (w-1)(m-wz) \bmod (p-1)$ כאשר z הוא הערך שחושב בסעיף ד. הוכיחו כי (w,δ) היא חתימה חוקית על m.

שאלה 3 [20 נקודות]

בין אליס לבוב ישנם שני ערוצי שידור. איב יכולה להאזין לערוץ אחד בלבד. יהי q מספר ראשוני. אליס רוצה לשלוח הודעה $m \in \mathbb{Z}_q$, כאשר כל הודעה $m \in \mathbb{Z}_q$ אפשרית.

סעיף א [4 נקודות]

כדי לשלוח הודעה $m \in \mathbb{Z}_q$, אליס מגרילה באקראי בהתפלגות אחידה $r_1 \in \mathbb{Z}_q$, מחשבת $r_2 \leftarrow (m + r_1) \bmod q$, שולחת r_1 בערוץ אחד ושולחת r_2 בערוץ השני.

הסבירו בקצרה מדוע איב היכולה להאזין רק לאחד מהערוצים אינה לומדת מידע על ההודעה שאליס שלחה.

סעיף ב [5 נקודות]

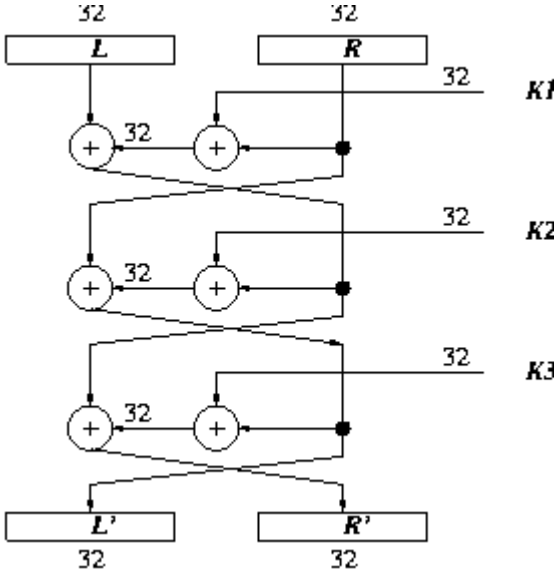
הסבירו מדוע בוב לא יכול לדעת אם איב שינתה את המידע שנשלח על אחד הערוצים.

סעיף ג [11 נקודות]

כדי להתגבר על הבעיה מסעיף ב, אליס מגרילה באקראי בהתפלגות אחידה חמש מחרוזות $r_1, a_1, b_1, a_2, b_2 \in \mathbb{Z}_q$, מחשבת $r_2 \leftarrow (m + r_1) \bmod q$, $c_1 \leftarrow (a_1 r_1 + b_1) \bmod q$ ו- $c_2 \leftarrow (a_2 r_2 + b_2) \bmod q$, שולחת r_1, c_1, a_2, b_2 בערוץ אחד ושולחת r_2, c_2, a_1, b_1 בערוץ השני. נתון כי איב יכולה להאזין לאחד מהערוצים ולשנות את המידע שנשלח בו. הוכיחו כי לא משנה איך איב תשנה את תוכן השידור, ההסתברות שבוב לא יוכל לזהות שינוי היא לכל היותר $1/q$.

שאלה 4 [26 נקודות]

בשאלה זו נראה איך לשבור מערכת הצפנה דמוית DES עם 3 סיבובים כאשר הפונקציה f מוחלפת ב- $\oplus$. ליתר דיוק, נעסוק במערכת הקריפטוגרפית המצוירת לעיל.



סעיף א [13 נקודות]

הראו כי בהינתן זוג קלט-פלט של המערכת $M=(L,R)$ ו- $C=(L',R')$ ישנם בדיוק 2^{32} אפשרויות למפתחות $k1,k2,k3$.

סעיף ב [13 נקודות]

נתון כי איב יודעת זוג קלט-פלט אחד של המערכת $M=(L,R)$ ו- $C=(L',R')$. הראו כי איב יכולה לפענח ביעילות כל קריפטוגרמה אחרת.